EXHIBIT "B"

Fulton County Superior Court
EFILEDWW
Date: 10/20/2015 4:20:44 PM
Cathelene Robinson, Clerk

IN THE SUPERIOR COURT OF FULTON COUNTY, GEORGIA

136 PRYOR STREET, ROOM C-103, ATLANTA, GEORGIA 30303

SUMMONS

PRINCIPLE SOLUTIONS GROUP, LLC

Plaintiff,

vs.

IRONSHORE INDEMNITY, INC

Defendant

Case No.: 2015CV267187

TO THE ABOVE NAMED DEFENDANT(S): Ironshore Indemnity, Inc. c/o Registered Agent: Corporation Service Company, 40 Technology Parkway South, Suite 300, Norcross, GA 30092

You are hereby summoned and required to file electronically with the Clerk of said Court at https://efilega.tylerhost.net/ofsweb and serve upon plaintiff's attorney, whose name and address is:

James J. Leonard
Barnes & Thornburg, LLP
3475 Piedmont Road, N.E., Suite 1700
Atlanta, Georgia 30305-2954

An answer to the complaint which is herewith served upon you, within 30 days after service of this summons upon you, exclusive of the day of service; unless proof of service of this complaint is not filed within five (5) business days of such service. Then time to answer shall not commence until such proof of service has been filed. **IF YOU FAIL TO DO SO, JUDGMENT BY DEFAULT WILL BE TAKEN AGAINST YOU FOR THE RELIEF DEMANDED IN THE COMPLAINT.**

This 10/21/2015 day of _____, 20 _____

Honorable Cathelene "Tina" Robinson
Clerk of Superior Court
By _____
Deputy Clerk

To defendant upon whom this petition is served:
This copy of complaint and summons was served upon you _____, 20_____

_____
Deputy Sherriff

Instructions: Attach addendum sheet for additional parties if needed, make notation on this sheet if addendum is used

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

PRINCIPLE SOLUTIONS GROUP, LLC,	)	
	)	
Plaintiff,	)	
	)	CIVIL ACTION FILE
v.	)	NO. 2015CV267187
	)	
IRONSHORE INDEMNITY, INC.,	)	**JURY TRIAL DEMANDED**
	)	
Defendant.	)	

COMPLAINT FOR BREACH OF CONTRACT AND BAD FAITH

COMES NOW, Principle Solutions Group, LLC ("Plaintiff" or "Principle"), and brings this cause of action for breach of insurance contract and insurance bad faith pursuant to O.C.G.A. § 33-4-6 against Ironshore Indemnity, Inc. ("Defendant" or "Ironshore"), and showing this Honorable Court as follows:

INTRODUCTION

1.

This is a civil action for breach of contract and bad faith brought by Principle. Principle is the insured under the crime insurance policy it bought from Ironshore. Among other coverages, Principle bought coverage in the crime insurance policy for Computer and Funds Transfer Fraud. Principle suffered a loss as a result of computer and funds transfer fraud. Ironshore denied coverage for the claim in full. Ironshore's denial of coverage is without any reasonable basis and Principle has been forced to bring this lawsuit to obtain the benefits it is due under the insurance policy. Principle also asserts that Ironshore acted in bad faith in refusing to provide any coverage under the crime insurance policy for Principle's losses resulting from a computer and funds transfer fraud in connection with a criminal and fraudulent computer-based event.

2.

Principle was the victim of an international wire transfer fraud. The crime was perpetrated by criminals who defrauded Principle through electronic instructions (in the form of emails and telephone calls) that purported to be issued from an employee of Principle and outside counsel for Principle, but were, in fact, fraudulently issued by someone else without the consent of Principle, the employee, or any outside counsel.

3.

The initial electronic instructions, purportedly from an executive within Principle, told a Principle employee to wire funds to cover the costs of a corporate transaction. Telephone instructions, purporting to be from attorneys for the company, confirmed the fraudulent instructions to wire money. Principle, based on these fraudulent instructions, directed its bank to wire funds. Principle suffered a $1,717,000 loss as a direct result of the fraud.

4.

Principle is the named insured under Commercial Crime Policy No. 001512502, a copy of which is attached hereto as Exhibit 1 and fully incorporated by reference (the "Policy"), which was issued and delivered by Ironshore in Georgia. The Policy specifically provides coverage for losses resulting from "Computer and Funds Transfer Fraud."

5.

Principle purchased the Policy, and the Policy is designed, to protect Principle against precisely the type of loss it has now incurred as a result of the fraudulent wire transfer. Yet despite the fact that Principle paid its premiums, gave prompt notice of the fraud to Ironshore, and cooperated fully and completely with Ironshore's inquiry into the fraud, Ironshore has failed

and refused to pay Principle's claim for coverage under the Policy (the "Claim"). This refusal to pay is groundless and constitutes a breach of Ironshore's contractual obligations.

6.

Principle seeks a declaration that there is coverage for the Claim under the Policy and damages for breach of contract due to Ironshore's unreasonable failure to honor its obligations under the Policy to cover the Claim.

7.

Ironshore has not paid any of Principle's Loss to date. On August 17, 2015, Principle, through undersigned counsel, sent to Ironshore a 60-day demand letter for $1,717,000 pursuant to O.C.G.A. § 33-4-6, demanding payment of the loss incurred.

8.

The 60-day period expired without Ironshore paying any of the loss demanded. The total amount of Principle's losses exceed the O.C.G.A. § 33-4-6 demand.

PARTIES, JURISDICTION AND VENUE

9.

Plaintiff Principle is a corporation organized under the laws of the State of Georgia with its principal place of business in Atlanta, Georgia.

10.

Upon information and belief, Defendant Ironshore is an insurance company organized under the laws of the State of New York with its principal place of business in New York, New York. Upon information and belief, Ironshore is authorized to sell or write insurance in Georgia and, at all material times, has conducted and continues to conduct substantial insurance business in the State of Georgia, including engaging in the business of selling insurance, investigating claims, and/or issuing policies that cover policyholders or activities located in Georgia.

11.

This Court has subject matter jurisdiction over this dispute, and the exercise of personal jurisdiction over the Defendant, who maintains corporate offices at Five Concourse Parkway, Suite 2700, Sandy Springs, Georgia 30328, would not offend traditional notions of fair play and substantial justice.

12.

Venue is proper in Fulton County, as Principle's offices are in Fulton County, the Defendant issued the Policy in this County, is located here, and many of the acts and omissions asserted herein occurred in this County.

THE IRONSHORE POLICY

13.

In consideration of significant premiums paid to cover exactly the type of loss at issue here, Ironshore sold the Policy to Principle for the policy period December 20, 2014 to December 20, 2015.

14.

The Policy provides coverage for a wide variety of criminal and fraudulent activities, including, but not limited to, "Computer and Funds Transfer Fraud."

15.

The Policy provides "Limits of Liability" for Computer and Funds Transfer Fraud Coverage of $5,000,000, subject to a $25,000 retention.

16.

The Policy provides, under Section A.6, "Computer and Funds Fraud Coverage," which states:

a. We will pay for:

(1) Loss resulting directly from a fraudulent:

(a) Entry of "electronic data" or "computer program" into; or

(b) Change of "electronic data" or "computer program" within;

(c) any "computer system" owned, leased or operated by you, provided the fraudulent entry or fraudulent change causes, with regard to Paragraphs 6.a.(1)(a) and 6.a.(1)(b):

(i) "Money," "securities" or "other property" to be transferred, paid or delivered; or

(ii) Your account at a "financial institution" to be debited or deleted.

(2) Loss resulting directly from a "fraudulent instruction" directing a "financial institution" to debit your "transfer account" and transfer, pay or deliver "money" or "securities" from that account.

b. As used in Paragraph 6.a.(1), fraudulent entry or fraudulent change of "electronic data" or "computer program" shall include such entry or change made by an "employee" acting, in good faith, upon a "fraudulent instruction" received from a computer software contractor who has a written agreement with you to design, implement or service "computer programs" for a "computer system" covered under this Insuring Agreement.

17.

The Policy further provides, under Section F.1:

a. "Computer program" means a set of related electronic instructions, which direct the operation and function of a computer or devices connected to it, which enable the computer or devices to receive, process, store or send "electronic data."

18.

The Policy provides, under Section F.2:

a. "Computer system" means:

(1) Computers, including Personal Digital Assistants (PDAs) and other transportable or handheld devices, electronic storage devices and related peripheral components;

(2) Systems and applications software; and

(3) Related communications networks;

(4) by which "electronic data" is collected, transmitted, processed, stored or retrieved.

19.

The Policy provides, under Section F.6:

a. "Electronic data" means information, facts, images or sounds stored as or on, created or used on, or transmitted to or from computer software (including systems and applications software) on data storage devices, including hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

20.

The Policy provides, under Section F.9:

a. "Financial institution" means:

(1) With regard to Insuring Agreement A.3.:

(a) A bank, savings bank, savings and loan association, trust company, credit union or similar depository institution; or

(b) An insurance company.

(2) With regard to Insuring Agreement A.6.:

(a) A bank, savings bank, savings and loan association, trust company, credit union or similar depository institution;

(b) An insurance company; or

(c) A stock brokerage firm or investment company.

21.

The Policy provides, under Section F.12:

a. "Fraudulent instruction" means:

(1) With regard to Insuring Agreement A.6.a.(2):

(a) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instruction directing a "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that "transfer

account", which instruction purports to have been issued by you, but which in fact was fraudulently issued by someone else without your knowledge or consent.

(b) A written instruction (other than those covered by Insuring Agreement A.2.) issued to a "financial institution" directing the "financial institution" to debit your "transfer account" and to transfer, pay or deliver "money" or "securities" from that "transfer account", through an electronic funds transfer system at specified times or under specified conditions, which instruction purports to have been issued by you, but which in fact was issued, forged or altered by someone else without your knowledge or consent.

(c) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or written instruction initially received by you, which instruction purports to have been issued by an "employee", but which in fact was fraudulently issued by someone else without your or the "employee's" knowledge or consent.

(2) With regard to Insuring Agreement A.6.b.:

(a) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic, written or voice instruction directing an "employee" to enter or change "electronic data" or "computer programs" within a "computer system" covered under the Insuring Agreement, which instruction in fact was fraudulently issued by your computer software contractor.

22.

The Policy provides, under Section F.16:

a. "Money" means:

(1) Currency, coins and bank notes in current use and having a face value;

(2) Traveler's checks and money orders held for sale to the public; and

(3) In addition, includes:

(a) Under Insuring Agreements A.1. and A.2., deposits in your account at any financial institution; and

(b) Under Insuring Agreement A.6., deposits in your account at a "financial institution"; and

(c) Under Insuring Agreement A.6, deposits in your account at a "financial institution" as defined in Paragraph F.9.b.

Principle is the Victim of a Fraud

23.

Principle is a high-performance, award-winning IT staffing and consulting firm that is committed to producing results for its clients, candidates and employees. Principle has two founders who serve as its managing directors.

24.

On July 8, 2015, at 9:10 a.m., an employee in Principle's Accounts Payable department ("Employee 1") received an email from a person purporting to be one of the two Principle managing directors (the "Faked Executive"). Unfortunately, the person who sent the email was a fraudster who had modified the email to appear as if it came from the Faked Executive. In the Faked Executive's email that was sent to Principle (via Employee 1), the Faked Executive instructed Principle (via Employee 1) to wire funds to cover the costs of a secret corporate transaction. This email insisted Employee 1 "treat the matter with the utmost discretion and deal solely with" the fraudster posing as an attorney for Principle (the "Faked Attorney"). Principle's managing director (whose identity was faked) was not in the office on the day of the fraudulent email.

25.

The email was altered so that the "From" line of the email showed an email address that appeared to be for the executive at Principle, making it appear as if it had actually been sent by the Principle executive.

26.

Later that morning, Employee 1 received an email from the Faked Attorney, purportedly at the instruction of the Faked Executive, with specific wire instructions, including the recipient of the funds, the address, bank address, account number, and SWIFT/BIC code. He informed Employee 1 that the Faked Executive asked him to contact Employee 1 and requested a number at which to contact her.

27.

At 10:15 a.m., Faked Attorney called to ask Employee 1 if the wire instructions were received and emphasized the importance of completing the wire transfer that day, adding that he, Faked Attorney, had Faked Executive's full approval to execute the wire. Faked Attorney also informed Employee 1 that she would need the assistance of her subordinate, ("Employee 2"), who would create the wire instructions to be approved by Employee 1.

28.

Employee 1 called Principle's bank (the "Financial Institution") to verify the process for international wires.

29.

Employee 1 was not able to forward an email to the Financial Institution to wire the funds.

30.

Under UCC § 4A-202, a bank must use a "security procedure" that is commercially reasonable to provide security against unauthorized payment orders.

31.

Under UCC § 4A-201, "[a] security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with an authorized specimen signature of the customer is not by itself a security procedure."

32.

The Financial Institution allows wires to be sent via a portal or mobile device app.

33.

Employee 1 logged into Principle's Financial Institution account to enable the approval function and verify the capability to wire internationally in different forms of currency. Employee 1 then emailed Faked Attorney to confirm capability.

34.

After Employee 1 reviewed the email sent by the Faked Attorney, at the behest of the Faked Executive, Employee 1 had Employee 2 create the wire instructions. Employee 1 later approved the wire instructions.

35.

Employee 1 received an email and phone call from the Financial Institution's fraud prevention unit regarding verification and purpose of the wire. The Financial Institution requested Employee 1 verify with Faked Attorney how he received the wire instructions. Employee 1 spoke to Faked Attorney, who said he received the wire instructions verbally from

Faked Executive. Employee 1 relayed this information to the Financial Institution and the Financial Institution then released the wire.

36.

The next day, Employee 1 spoke to the actual managing director (who was the Faked Executive in the emails) to confirm that the wire had been made in accordance with his (fraudulent) instruction.

37.

After Employee 1 completed the wire instructions and the wire was completed, Employee 1 spoke in person with the actual Faked Executive to confirm that she had sent the instructions in accordance with his request. The actual Faked Executive had no knowledge of the emails, Faked Attorney, or wire instruction, and immediately called the fraud department of the Financial Institution to report the computer and funds transfer fraud.

38.

Principle reported the fraud to the authorities, but the identity of the person(s) who acted as the Faked Executive and Faked Attorney have not been discovered and the transferred funds were not recovered.

Ironshore's Denial of Coverage

39.

Principle promptly notified Ironshore of the fraudulent wire and made the Claim for coverage under the Policy.

40.

Ironshore acknowledged receipt of the Claim.

41.

Coverage exists under the Computer and Funds Transfer Fraud Coverage.

42.

Principle suffered a covered Loss of $1,717,000.

43.

There was a "fraudulent instruction." There were computer, telephone, or other electronic instructions, initially received by Principle, that purported to have been issued by an employee, but which, in fact, were issued by someone else, without Principle's consent.

44.

The fraudulent instruction(s) directed a "financial institution" to debit a transfer account and transfer, pay, or deliver money from that account. There were computer, telephone, or other electronic instructions to have a bank wire money.

45.

The phrase "resulting directly from" relates to whether the amount of losses that Principle suffered was an actual present loss, as distinguished from a theoretical or bookkeeping loss, and as distinguished from potential civil liability.

46.

The loss that Principle suffered was an actual present loss.

47.

The loss that Principle suffered was not a theoretical loss.

48.

The loss that Principle suffered was not a bookkeeping loss.

49.

The loss that Principle suffered was not potential civil liability.

50.

Alternatively, the question of direct loss is analogous to proximate cause.

51.

Principle's loss would not have occurred but for the fraudulent instruction(s).

52.

Principle's loss would not have occurred but for "A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or written instruction initially received by [Principle], which instruction purports to have been issued by an 'employee', but which in fact was fraudulently issued by someone else without [Principle's] or the 'employee's' knowledge or consent."

53.

On July 24, 2015 Ironshore denied coverage on the basis that the messages purportedly from the Faked Executive and on behalf of the Faked Executive "may not be characterized as 'directing a "financial institution" to debit your "transfer account" and transfer, pay or deliver "money" or "securities" from that account....'"

54.

Ironshore's denial letter demonstrates that the Policy language is either ambiguous or, if Ironshore's interpretation were correct, offers nothing but illusory coverage.

55.

Coverage under § 6.a.(2) states that Ironshore "will pay for . . . Loss resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit your 'transfer account' and transfer, pay or deliver 'money' or 'securities' from that account."

56.

A fraudulent instruction requires the communication to have been "initially received by you [Principle]."

57.

Ironshore's denial letter states that the fraudulent instruction did not direct the Financial Institution to wire money.

58.

Thus, under Ironshore's interpretation of the policy language in its denial letter, a fraudulent instruction must direct a bank to wire funds, but also have been received by the policyholder first. This result is logically impossible.

59.

Under Ironshore's interpretation of the policy language in its denial letter, the policyholders must receive the fraudulent email, facsimile, or telephone call, and the policyholder must forward the fraudulent email, facsimile, or telephone call to the bank, and the bank must follow the instructions to wire funds.

60.

Such an interpretation shows the ambiguity or illusory coverage in § 6.a.(2).

61.

A bank will not wire funds based on an email, facsimile, or telephone call alone, and certainly not from a third party.

62.

It is not commercially reasonable security for a bank to wire funds based on an email, facsimile, or telephone call alone.

63.

It would violate UCC § 4A-201 to accept a forwarded email, facsimile, or telephone call as a sufficient basis to wire money.

64.

Therefore, it is not a reasonable interpretation of the policy language to require Principle to have received the fraudulent instruction first, forwarded it to the Financial Institution, and have the Financial Institution make a wire transfer as a result.

65.

It is a reasonable interpretation of the policy language to require Principle to have received the fraudulent instruction first, and then act in accordance with the Financial Institution's portal for wire transfers to have the wire transfer be made.

66.

If Ironshore only will provide coverage for fraudulent wire transfers when a condition precedent cannot be met (under UCC § 4A-201 or the commercial practice of every major bank), then it would be commercially impossible for Ironshore's coverage to apply. That would mean Ironshore sold Principle illusory coverage, a result inconsistent with well-established Georgia law.

67.

When Ironshore denied coverage for the Claim, stating that coverage was not available under the Computer and Funds Transfer Fraud Coverage, Ironshore breached its contractual obligations to Principle and did so without any reasonable basis.

68.

Ironshore's denial of coverage was in bad faith because it was without substantial justification and in bad faith. Ironshore's coverage position is unreasonable and would prevent the policy from providing coverage for any fraudulent wire transfer because it would be impossible factually to meet the language as Ironshore has interpreted it.

FIRST CAUSE OF ACTION
(Breach of Contract)

69.

Plaintiff repeats and re-alleges the allegations set forth in paragraphs 1 through 68 of this Complaint as if fully set forth herein and incorporates same by reference.

70.

The Policy constitutes a valid and enforceable contract between Ironshore and Principle.

71.

Principle was the named insured under the Policy.

72.

Principle has paid all premiums, provided prompt notice of the Claim, and otherwise performed all conditions precedent and other obligations required of it under the Policy.

73.

Under the terms of the Policy, Ironshore must pay up to $5,000,000 for a direct loss of Money that comes within the Policy definitions of Computer and Funds Transfer Fraud.

74.

As detailed above, the facts of the Claim trigger coverage under the terms of the Policy.

75.

Ironshore has not paid any amount to Principle in connection with the Claim. By failing to provide coverage for the Claim, Ironshore has breached the terms of the Policy.

76.

As a direct and proximate result of Ironshore's breach of the Policy, Principle has suffered damages in an amount to be determined at trial, plus consequential damages, attorneys' fees, costs, and pre- and post-judgment interest, as well as any further damages and relief as the Court deems just and proper and available under applicable law.

SECOND CAUSE OF ACTION
(Insurance Bad Faith Pursuant To O.C.G.A. § 33-4-6)

77.

Plaintiff repeats and re-alleges the allegations set forth in paragraphs 1 through 76 of this Complaint as if fully set forth herein and incorporates same by reference.

78.

On August 17, 2015, Principle made the requisite 60-day demand pursuant to O.C.G.A. § 33-4-6, demanding that Ironshore pay the amount of $1,717,000 within 60 days of receipt of the demand.

79.

On September 3, 2015, Ironshore denied coverage for Principle's aforementioned loss without substantial justification and in bad faith.

80.

Ironshore's failure to pay the subject loss under the circumstances constitutes insurance bad faith, subjecting Ironshore to an additional 50% penalty of the unpaid loss plus Principle's attorney's fees and costs incurred in bringing this action. Principle seeks all such damages as allowed by law, as well as any further damages and relief as the Court deems just and proper and available under applicable law.

PRAYER FOR RELIEF

WHEREFORE, PREMISES CONSIDERED, Principle seeks all of its direct, consequential, and all other damages as permitted by law and in amounts to be proven at trial as set forth herein, in addition to a 50% penalty and attorney's fees as allowed by O.C.G.A. § 33-4-6. Principle also seeks pre- and post-judgment interest as permitted by law, as the Court deems just and proper and available under applicable law, as well as all other and further relief to which it may be justly entitled.

JURY DEMAND

Principle demands a trial by jury on all issues so triable.

Respectfully submitted this 20th day of October, 2015.

s/ James J. Leonard
James J. Leonard
Georgia Bar No. 446655
Barnes & Thornburg LLP
3475 Piedmont Road, N.E., Suite 1700
Atlanta, Georgia 30305-2954
(404) 264-4060 Telephone
(404) 264-4033 Facsimile
jim.leonard@btlaw.com

Attorneys for Plaintiff

Of Counsel:
Scott N. Godes (*Pro Hac Vice* application to be submitted)
BARNES & THORNBURG LLP
1717 Pennsylvania Ave., NW
Washington, DC 20006
Telephone: (202) 289-1313
Facsimile: (202) 289-1330
sgodes@btlaw.com

Carrie M. Raver (*Pro Hac Vice* application to be submitted)
BARNES & THORNBURG LLP
110 E. Wayne Street, Suite 600
Fort Wayne, IN 46802
Telephone: (260) 425-4652
Facsimile: (260) 424-8316
carrie.raver@btlaw.com